L3 Algèbre. Exercices. Polynômes irréductibles et extensions de corps

Polynômes irréductibles

1) Déterminer les racines dans $\mathbb{C}$ du polynôme $X^4 + X^2 + 1$.
Ce polynôme est-il irréductible sur $\mathbb{Q}$?

2) Le polynôme $X^4 + 4X^2 + 2$ est-il irréductible sur $\mathbb{Q}$?
Est-il irréductible sur $\mathbb{Q}(\sqrt{2})$?

3) a) Montrer que dans $\mathbb{F}_2[X]$ il n'y a qu'un seul polynôme irréductible de degré 2 qui est $X^2 + X + 1$.
b) Trouver tous les polynômes irréductibles de degré 4 dans $\mathbb{F}_2[X]$.
c) Le polynôme $X^5 + 3X^2 + X + 5$ est-il irréductible sur $\mathbb{Q}$?

4) a) Quelles sont les racines dans $\mathbb{C}$ du polynôme $X^4 + 1$?
b) Le polynôme $X^4 + 1$ est-il irréductible sur $\mathbb{R}$?
c) Montrer que si $X^4 + 1 = A(X)B(X)$ avec des polynômes $A(X)$ et $B(X)$ dans $\mathbb{Q}[X]$ de degré ≥ 1, alors le polynôme $X^2 + 2\sqrt{2}X + 1$ divise $A(X)$ ou $B(X)$ dans $\mathbb{R}[X]$. En déduire que X^4+1 est irréductible sur $\mathbb{Q}$. Retrouver ce résultat en utilisant le critère d'Eisenstein.
d) Soit p un nombre premier tel que -1 est un carré dans $\mathbb{F}_p$, trouver un tel p. Montrer que $X^4 + 1$ est réductible dans $\mathbb{F}_p[X]$.
e) Soit p un nombre premier tel que 2 ou -2 est un carré dans $\mathbb{F}_p$, trouver un tel p. Montrer que $X^4 + 1$ est réductible dans $\mathbb{F}_p[X]$.
(écrire $X^4 + 1 = (X^2 + 1)^2 - 2\ X^2$ ou $X^4 + 1 = (X^2 - 1)^2 - 2\ X^2$)
f) Montrer que $X^4 + 1$ est réductible dans $\mathbb{F}_p[X]$ pour tout nombre premier p.

5) a) Montrer que pour tout nombre premier p on a: p divise C_p^k pour tout $k = 1, ..., p - 1$.
Développer $(a + b)^p$ et $(a - b)^p$ dans $\mathbb{F}_p$. Développer $(a + b + c)^p$ dans $\mathbb{F}_p$.
b) Développer $(X^3 - 2X + 1)^5$ dans $\mathbb{F}_5[X]$.
c) Décomposer $X^{15} - 2X^5 + 1$ en facteurs irréductibles dans $\mathbb{F}_5[X]$.

Extensions de corps

1) a) Est-ce que le corps $\mathbb{R}$ est une extension de $\mathbb{F}_p$?

b) Soient $p < q$ deux nombres premiers, est-ce que le corps $\mathbb{F}_q$ est une extension de $\mathbb{F}_p$?

2) a) Soit $j = e^{\frac{2i\pi}{3}} = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$. Montrer que $1 + j + j^2 = 0$.

Quel est le polynôme minimal de j sur $\mathbb{Q}$?

b) L'extension $\mathbb{Q} \hookrightarrow \mathbb{Q}(j)$ est-elle algébrique?

Est-ce que $\sqrt{3} \in \mathbb{Q}(j)$? Est-ce que $j \in \mathbb{Q}(\sqrt{3})$?

c) Quel est le polynôme minimal de j sur $\mathbb{Q}(\sqrt{3})$?

Quel est le degré de l'extension $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{3},j)$?

Donner une base de $\mathbb{Q}(\sqrt{3},j)$ sur $\mathbb{Q}$.

d) Quel est le degré de l'extension $\mathbb{Q}(j) \hookrightarrow \mathbb{Q}(\sqrt{3}, j)$?

e) Est-ce que $i \in \mathbb{Q}(j)$? Est-ce que $i \in \mathbb{Q}(\sqrt{3},j)$?

Montrer que $\mathbb{Q}(\sqrt{3},j) = \mathbb{Q}(\sqrt{3},i)$.

f) Soit $\alpha = i + \sqrt{3}$. Calculer $(\alpha - i)^2$ et $(\alpha - \sqrt{3})^2$. Montrer que $\sqrt{3} \in \mathbb{Q}(i + \sqrt{3})$ et $i \in \mathbb{Q}(i + \sqrt{3})$. Montrer que $\mathbb{Q}(\sqrt{3},i) = \mathbb{Q}(i + \sqrt{3})$.

3) a) Soit $P(X) = X^3 + 2X + 2$, montrer que P est irréductible sur $\mathbb{Q}$.

b) Montrer qu'il existe une seule racine réelle α de ce polynôme. Cette racine est-elle rationelle?

c) L'extension $\mathbb{Q} \hookrightarrow \mathbb{Q}(\alpha)$ est-elle de degré fini? est-elle algébrique?

Donner une base de $\mathbb{Q}(\alpha)$ sur $\mathbb{Q}$.

Exprimer $\frac{1}{\alpha}$, dans cette base. Exprimer $\frac{1}{1+\alpha+\alpha^2}$ dans cette base.

d) Soit $\beta \in \mathbb{Q}(\alpha)$ avec $\beta \notin \mathbb{Q}$. Quel est le degré de l'extension $\mathbb{Q} \hookrightarrow \mathbb{Q}(\beta)$?

Donner le polynôme minimal sur $\mathbb{Q}$ de $\beta = 1 + \alpha$.

4)a) Soit $P(X) = X^2 + X - 1$, montrer que P est irréductible sur $\mathbb{F}_3$.

b) Soit le corps $L = \mathbb{F}_3[X]/(P)$. Montrer que L est une extension de $\mathbb{F}_3$.

c) Soit $\alpha = \widehat{X} \in L$. Montrer que α est algébrique sur $\mathbb{F}_3$. Quel est son polynôme minimal sur $\mathbb{F}_3$? Quel est le conjugué de α dans L?

d) Montrer que tout élément de L s'écrit $a + b\alpha$ avec a et b dans $\mathbb{F}_3$. Ecrire tous les éléments de L avec la représentation $\mathbb{F}_3 = \{0, 1, -1\}$.

e) Vérifier que tout élément de L s'écrit α^k où $k = 0, 1, ..., 7$.

L3 Algèbre. Polynômes irréductibles et extensions de corps. Indications sur les exercices.

Polynômes irréductibles

1) Ecrire $X^4+X^2+1=X^4+2X^2+1-X^2$

2) Eisenstein et poser $Y=X^2$

3) a) Si $P\in K[X]$ est un polynôme de degré 2 ou 3 on a:
P polynôme irréductible sur $K \Leftrightarrow P$ n'a pas de racines dans K.
b) On a :
P irréductible sur $K \Rightarrow P$ n'a pas de racine dans K
Donc on commence par chercher les polynômes de degré 4 dans $\mathbb{F}_2[X]$ et sans racine dans $\mathbb{F}_2$ ensuite on remarque que P ne peut avoir un facteur de degré 1 et on utilise a).
c) On réduit modulo 2

4) a) Les racines de X^4+1 dans $\mathbb{C}$ sont $\pm\frac{1}{2}\sqrt{2}\pm\frac{1}{2}i\sqrt{2}$
b) On a $(X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1)=X^4+1$
c) Le polynôme $(X^2+\sqrt{2}X+1)$ n'a pas de racine dans $\mathbb{R}$ et est de degré 2, donc il est irréductible sur $\mathbb{R}$. Si $X^4+1=A(X)B(X)$ avec $A(X)$ et $B(X)$ dans $\mathbb{Q}[X]$ de degré ≥ 1 alors $A(X)$ et $B(X)$ sont de degré 2 (pourquoi ?), on aurait par exemple $A(X)=c(X^2+\sqrt{2}X+1)$ avec $c\in\mathbb{R}$ ce qui n'est pas possible.
Développer $(X+1)^4+1$ et utiliser le critère d'Eisenstein.
d) Par exemple $p=5$ $(-1=2^2)$, alors

$$X^4+1=X^4-(-1)=X^4-a^2=(X^2+a)(X^2-a)$$

e) Par exemple $p=7$ $(2=4^2)$

$$X^4+1=(X^2+1)^2-2X^2=(X^2+1)^2-a^2X^2$$

f) Si -1 et 2 ne sont pas des carrés dans $\mathbb{F}_p$ alors leur produit est un carré dans $\mathbb{F}_p$ (voir la caractérisation des carrés dans $\mathbb{F}_p$)

5) a) On a

$$k!C_p^k=p(p-1)...(p-k+1)$$

donc p divise $k!C_p^k$.
On a

$$(a+b)^p=a^p+\sum_{k=1}^{p-1}C_p^k a^k b^{p-k}+b^p$$

et $(a+b+c)^p=((a+b)+c)^p$
b)

$$(X^3-2X+1)^5=X^{3.5}-2^5X^5+1^5$$

c) X^3-2X+1 a une racine évidente qui est 1 donc il est divisible par $X-1$.

Extensions

1) Dans $\mathbb{F}_p$ on a $p.1_{\mathbb{F}_p} = 0$ et si f est un morphisme de $\mathbb{F}_p$ dans K alors

$$f(p.1_{\mathbb{F}_p}) = p.f(1_{\mathbb{F}_p}) = p.1_K$$

2) a) Le polynôme $X^2 + X + 1$ est irréductible sur $\mathbb{Q}$.

b) L'extension $\mathbb{Q} \hookrightarrow \mathbb{Q}(j)$ est de degré 2. Si $\sqrt{3} \in \mathbb{Q}(j)$ alors on aurait $\sqrt{3} = a+bj$ avec a et b dans $\mathbb{Q}$.

c) Le polynôme $X^2 + X + 1$ est irréductible sur $\mathbb{Q}(\sqrt{3})$. Le degré de l'extension $\mathbb{Q} \hookrightarrow Q(\sqrt{3}, j)$ s'obtient par le théorème de multiplicativité des degrés.

Une base de $\mathbb{Q}(\sqrt{3}, j)$ sur $\mathbb{Q}$: $1, \sqrt{3}, j, j\sqrt{3}$

d) $\deg(\mathbb{Q} \hookrightarrow Q(\sqrt{3}, j))$=$\deg(\mathbb{Q} \hookrightarrow \mathbb{Q}(j))$ $\deg(\mathbb{Q}(j) \hookrightarrow Q(\sqrt{3}, j))$

e) Si $i \in \mathbb{Q}(j)$ alors on aurait $i = a+bj$ avec a et b dans $\mathbb{Q}$ donc $i = a - b\frac{1}{2} + ib\frac{\sqrt{3}}{2}$.

On a $j = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$ donc $i = 2\frac{j+\frac{1}{2}}{\sqrt{3}}$

f) On a $\alpha^2 - 2i\alpha - 1 = 3 \Rightarrow i = \frac{4-\alpha^2}{-2\alpha}$ et $\alpha^2 - 2\alpha\sqrt{3} + 3 = -1 \Rightarrow \sqrt{3} = \frac{-4-\alpha^2}{-2\alpha}$.

Donc $\mathbb{Q}(\sqrt{3},i) \subset \mathbb{Q}(i + \sqrt{3})$.

3) a) Utiliser Eisenstein

b) Etudier la fonction $x \mapsto x^3 + 2x + 2$. Si $\alpha \in \mathbb{Q}$ alors P serait divisible par $(X - \alpha)$.

c) L'extension $\mathbb{Q} \hookrightarrow \mathbb{Q}(\alpha)$ est de degré 3. Une base: $1,\alpha, \alpha^2$.

On a $\alpha^3 + 2\alpha + 2 = 0$ donc

$$\alpha(\alpha^2 + 2) = -2 \Rightarrow \frac{1}{\alpha} = \frac{(\alpha^2 + 2)}{-2} = -1 + (\frac{-1}{2})\alpha^2$$

Les polynômes $M_\alpha(X) = X^3 + 2X + 2$ et $A(X) = X^2 + X + 1$ sont premiers entre eux dans $\mathbb{Q}[X]$, on écrit la relation de Bezout:

$$UM_\alpha + VA = 1$$

ce qui donne $V(\alpha)A(\alpha) = 1$ donc $\frac{1}{1+\alpha+\alpha^2} = V(\alpha)$.

d) Ecire $\alpha = \beta - 1$.

4) a) $X^2 + X - 1$ ne s'annule pas sur $\mathbb{F}_3$.

b) L'application

$$\mathbb{F}_3 \to \mathbb{F}_3[X] \to \mathbb{F}_3[X]/(P)$$

est un morphisme. Comme P est irréductible sur $\mathbb{F}_3$alors $\mathbb{F}_3[X]/(P)$ est un corps.

c) On a

$$\alpha^2 + \alpha + 1 = \widehat{X}^2 + \widehat{X} - 1 = \widehat{X^2 + X} - 1 = 0$$

On a $X^2 + X - 1 = (X - \alpha)Q(X)$ d'où $Q(X)$ de degré 1 donc $Q(X) = aX + b$ et on identifie.

d) On écrit $L = \{0, 1, -1, \alpha, -\alpha, \alpha + 1, -\alpha - 1, -\alpha + 1, \alpha - 1\}$

e) $\alpha^2 = -\alpha + 1$,

$\alpha^3 = \alpha(-\alpha + 1) = -\alpha^2 + \alpha = \alpha - 1 + \alpha = -1 + 2\alpha = -1 - \alpha$,

...